MAY 0 1 2007

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

The Honorable Stewart A. Baker
Assistant Secretary for Policy
Department of Homeland Security
Washington, DC 20528

The Honorable Henrietta H. Fore
Under Secretary for Management
Department of State
Washington, DC 20520

Dear Mr. Baker and Ms. Fore:

Pursuant to Section 546 of the Homeland Security Appropriations Act of 2007 (P.L. 109-295), the National Institute of Standards and Technology (NIST) has reviewed the card architecture of the Western Hemisphere Travel Initiative PASS Card proposed by the Department of State.

Section 546 requires NIST to certify that "the Departments of Homeland Security and State have selected a card architecture that meets or exceeds International Organization for Standardization (ISO) security standards and meets or exceeds best available practices for protection of personal identification documents." Subsequent to the passage of the Homeland Security Appropriations Act of 2007, the Departments of State and Homeland Security reached agreement on the choice of the technology for the PASS Card which is called "Gen 2 RFID." Given this agreement between the Departments of State and Homeland Security, NIST focused its efforts on working with the two agencies to assure that the Gen 2 RFID met the requirements of Section 546.

Card architecture has been interpreted by NIST to encompass the physical ID card itself, particularly: the information printed on the card, including its overall layout, logos, images, etc.; the information encoded in the machine readable zone; the information in the RFID chip; the information available by inspecting tamper-evident or anti-counterfeiting security features; and the specific physical features of the card that protect and deliver the information content. While not necessarily part of the physical card, the proposed RF attenuation sleeve has been considered part of the architecture since it is necessary to mitigate the tracking risk if an activation switch is not employed.

NIST identified the following ISO standards as being relevant to the PASS Card architecture, for the Gen 2 RFID (Radio Frequency Identification) technology chosen by the Departments of State and Homeland Security:

(a) ISO/IEC 7810, Identification cards - Physical characteristics
(b) ISO 18047-6, Parameters for Air Interface Communications at 860 to 960 MHz
(c) ISO 15408-1, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

NIST

(d) ISO 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
(e) ISO 15693-1, Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 1: Physical characteristics
(f) ISO 17799, Information technology - Security techniques - Code of practice for information security management
(g) ISO 18000-6:2004/Amd.1:2006(E), Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz, AMENDMENT 1: Extension with Type C and update of Types A and B
(h) ISO 10373-1, Identification cards - Test methods - Part 1: General characteristics tests
(i) ISO 10373-6, Improved RF test methods

NIST identified the following best available practices and non-ISO standards for protection of personal identification documents, for the technology chosen by the Departments of State and Homeland Security:

(j) "Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft)," Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Phillips. NIST Special Publication SP 800-98, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce
(k) "Recommended Security Controls for Federal Information Systems," Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers. NIST Special Publication SP800-53, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, September 2006.
(l) "The Use of RFID for Human Identity Verification," Report No. 2006-02, Data Privacy & Integrity Advisory Committee to the Secretary and Chief Privacy Officer of the Department of Homeland Security, adopted December 6, 2006.
(m) "CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology." http://www.cdt.org/privacy/20060501rfid-best-practices.php.
(n) "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
(o) "RFID and Security," Sanjay Sarma, invited presentation for Workshop on RFID Security 2006.
(p) EPC Radio-Frequency Identity Protocols Class-1 Generation 2 UHF RFID Conformance Requirements Version 1.0.2
(q) The EPCglobal Architecture Framework - EPCglobal Final Version of July 1, 2005
(r) EPCglobal Class-1 Generation-2 UHF RFID
(s) EPCglobal Tag Data Standards Version 1.3
(t) ICAO 9303 Part 3 Volume 1 Section IV recommendations for TD-1 Documents of Identity

NIST also considered best practices that it had developed when testing the physical security of the U.S. Passport prototypes in the past.

After reviewing the attached documents - Sections C, J, and M from the draft Request for Proposals (RFP) as amended on April 30, 2007 submitted by the Departments of State and Homeland Security - and analyzing them against the standards and best practices cited above, NIST has determined - and I therefore certify - that this proposed card architecture as described in Sections C, J, and M from the draft RFP as amended on April 30, 2007, meets or exceeds the relevant standards and best practices as specified in the statute, for the technology chosen by the Departments of State and Homeland Security.

For internal consistency we also paid special attention to the privacy recommendations from the Data Privacy & Integrity Advisory Committee to the Secretary and Chief Privacy Officer of the Department of Homeland Security. Attachment C provides some additional comments related specifically to DHS Report No. 2006-02 prepared by this committee.

I note that the Departments made a variety of changes in the details of the technical approach for the PASS Card based upon discussions among NIST, State, and the Department of Homeland Security technical representatives. These changes have improved the security of the card architecture. I am pleased that this has been a cooperative effort resulting in what we believe is a more rigorous approach for the PASS Card. See Attachment B (Section I).

Please note that this certification applies only to the security of the card architecture, as specified in the statute. We have not tested any functioning PASS Cards or RF attenuation sleeves as part of our analysis. We have reviewed broader security, reliability, and interoperability considerations of the PASS Card and have offered suggestions to your staff that could further improve these aspects of the Card. Those additional suggestions are outside of the scope of our certification and were not taken into consideration during our review. See Attachment B (Section II).

It is our intention to notify the House and Senate Appropriations Subcommittees on Homeland Security promptly that we have completed this work and that we have certified the card architecture following the statutes directions.

Sincerely,

William Jeffrey

William Jeffrey
Director

Attachments
A. State/DHS documents reviewed by NIST for certification (3)
B. NIST Changes Required for Certifying the Security of PASS Card Architecture or Recommended for Improvement in Interoperability and Performance
C. NIST Analysis of DHS Report No. 2006-02

NOTE: Attachments are procurement sensitive and not publicly reviewable at this time.